

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-312261

(43)Date of publication of application : 25.10.2002

(51)Int.Cl.

G06F 13/00
H04L 12/66

(21)Application number : 2001-110528

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>

(22)Date of filing : 09.04.2001

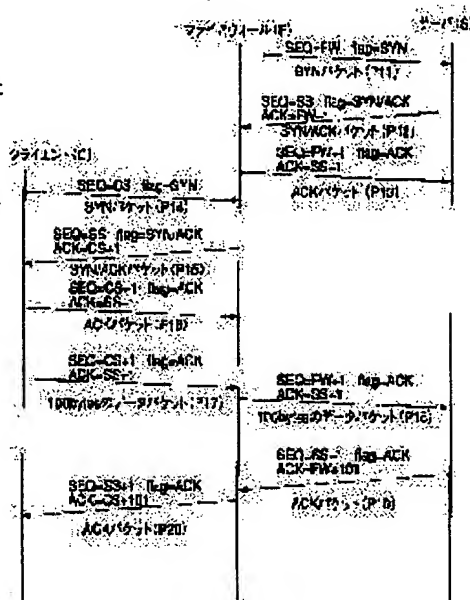
(72)Inventor : KAJIWARA FUMIO
OKABE KEIICHI
MORIAI SATOSHI

(54) NETWORK SERVICE RELAY METHOD AND RELAY DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To construct a firewall having both performance deciding up to justice of a service request similarly to an 'application gateway' and shortness of a response time equivalent to 'packed filtering'.

SOLUTION: In the fire wall (F), connection between the firewall (F) and a server (S) is previously established to the server (S) and is managed. Thereby, a connection load to the server (S) when a client (C) requests connection is reduced, and speed-up relay processing is realized by only rewriting an SEQ number and an ACK number when relaying TCP data packets between the server (S) and the client (C). The firewall (F) has a function of verifying the justice in the case of service request transfer, and cuts off injustice request transfer.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

BEST AVAILABLE COPY

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号 ✓
特開2002-312261
(P2002-312261A)

(43) 公開日 平成14年10月25日 (2002. 10. 25)

(51) Int.Cl. ⁷	識別記号	F I	フォーマット* (参考)
G 0 6 F 13/00	3 5 3	G 0 6 F 13/00	3 5 3 C 5 B 0 8 9
	3 5 1		3 5 1 Z 5 K 0 3 0
H 0 4 L 12/66		H 0 4 L 12/66	B

審査請求 未請求 請求項の数18 O L (全 13 頁)

(21) 出願番号 特願2001-110528 (P2001-110528)

(22) 出願日 平成13年4月9日 (2001. 4. 9)

(71) 出願人 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(72) 発明者 梶原 史雄

東京都千代田区大手町二丁目3番1号 日

本電信電話株式会社内

(72) 発明者 岡部 恵一

東京都千代田区大手町二丁目3番1号 日

本電信電話株式会社内

(74) 代理人 100058479

弁理士 鈴江 武彦 (外2名)

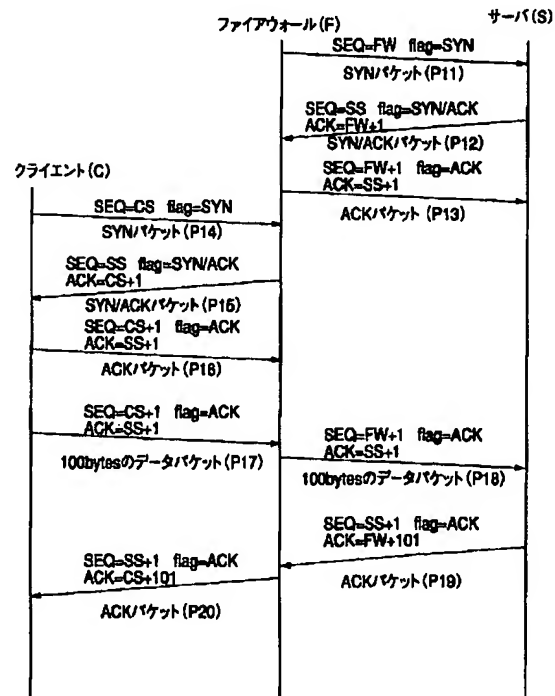
最終頁に続く

(54) 【発明の名称】 ネットワークサービス中継方法及び中継装置

(57) 【要約】

【課題】 「アプリケーション・ゲートウェイ」と同様にサービス要求の正当性まで判断する能力と「パケット・フィルタリング」と同等の応答時間の短さを兼ね備えるファイアウォールを構築する。

【解決手段】 ファイアウォール (F) において、予めサーバ (S) との間でファイアウォール-サーバ間コネクションを確立し、管理しておくことで、クライアント (C) からのコネクション要求時のサーバ (S) への接続負荷を軽減し、サーバ (S) とクライアント (C) との間のTCPデータパケット中継時にはSEQ番号およびACK番号の書き換えのみとすることで、中継処理の高速化を実現する。さらにサービス要求転送時に正当性を検証する機能を持たせ、不正な要求転送を遮断する。



【特許請求の範囲】

【請求項1】 任意の二つのコンピュータ間でのコネクションを双方のコネクションキーに基づいて確立可能なネットワークに適用され、あるコンピュータ上のサーバによって提供されるサービスを、そのコンピュータとは別のコンピュータ、もしくは同一のコンピュータによって提供されるファイアウォールを介して、他のコンピュータ上のクライアントに提供するネットワークサービス中継方法であって、

前記ファイアウォールと前記サーバとの間に予め1本以上のファイアウォールサーバ間コネクションを確立し、前記コネクションに用いられた前記サーバ側と前記ファイアウォール側のコネクションキーを保持しておく第1のステップと、

前記クライアントと前記ファイアウォールとの間に第1のステップで保持しておいた前記サーバ側コネクションキーの一つを用いてクライアントファイアウォール間コネクションを確立し、前記コネクションの確立に用いられた前記クライアント側のコネクションキーと前記ファイアウォール側のコネクションキーを保持する第2の

ステップと、
前記クライアントファイアウォール間コネクションと前記ファイアウォールサーバ間コネクションとを結合・中継する第3のステップとを具備することを特徴とするネットワークサービス中継方法。

【請求項2】 前記第3のステップは、前記クライアントから届くメッセージのコネクションキーを前記ファイアウォールサーバ間コネクションの前記ファイアウォール側のコネクションキーに書き換えて前記サーバへ転送し、前記サーバから届くメッセージのコネクションキーを前記クライアントファイアウォール間コネクションの前記クライアント側のコネクションキーに書き換えて前記クライアント側へ転送することを特徴とする請求項1に記載のネットワークサービス中継方法。

【請求項3】 前記第1のステップは、予め管理収容本数として整数 M ($M \geq 1$) が指定されているとき、前記クライアントファイアウォール間コネクションと未結合のファイアウォールサーバ間コネクションと、クライアントファイアウォール間コネクションと結合済みのファイアウォールサーバ間コネクションを合わせた、ファイアウォールサーバ間コネクションの合計が M 本以下となるように、ファイアウォールサーバ間コネクションの確立を制限することを特徴とする請求項1に記載のネットワークサービス中継方法。

【請求項4】 前記第1のステップは、予め初期の管理収容本数として整数 N ($M \geq N \geq 1$) が指定されているとき、初期状態で N 本の未結合ファイアウォールサーバ間コネクションを確立する初期化処理を実行することを特徴とする請求項3に記載のネットワークサービス中継方法。

【請求項5】 前記第1のステップは、前記ファイアウォールサーバ間コネクションの合計が M 本以下のとき、前記未結合ファイアウォールサーバ間コネクションの切断または前記クライアントファイアウォール間コネクションとの結合により前記未結合ファイアウォールサーバ間コネクションが N 本より少なくなった場合に、新たに未結合ファイアウォールサーバ間コネクションを確立して、 N 本の未結合ファイアウォールサーバ間コネクションを維持することを特徴とする請求項4に記載のネットワークサービス中継方法。

【請求項6】 前記第2のステップは、前記ファイアウォールサーバ間コネクションと結合していない未結合のクライアントファイアウォール間コネクションと、前記ファイアウォールサーバ間コネクションと結合済みのファイアウォールクライアント間コネクションとを合わせた、クライアントファイアウォール間コネクションの合計が、前記第1のステップで確立されている前記ファイアウォールサーバ間コネクションの合計を上回らないように、クライアントファイアウォール間コネクションの確立を制限することを特徴とする請求項1に記載のネットワークサービス中継方法。

【請求項7】 前記第2のステップは、新たにクライアントからファイアウォールに対してコネクション確立要求があった場合に、前記未結合ファイアウォールサーバ間コネクションの数と前記未結合クライアントファイアウォール間コネクションの数を比較し、サーバ側コネクション数よりクライアント側コネクション数が上回っていれば、新たにクライアントファイアウォール間コネクションを確立し、

クライアント側コネクション数がサーバ側コネクション数と同数か下回るようであれば、クライアントからのコネクション確立要求を廃棄するか、あるいは、前記未結合ファイアウォールサーバ間コネクションの数が前記未結合クライアントファイアウォール間コネクションの数を上回るまでクライアントファイアウォール間コネクション確立を遅延することを特徴とする請求項1に記載のネットワークサービス中継方法。

【請求項8】 前記第3のステップは、前記クライアントファイアウォール間コネクションとファイアウォールサーバ間コネクションとの結合状態で、前記クライアントファイアウォール間コネクションを通じて前記クライアントからのメッセージを受信した場合に、このメッセージを検証して不正の有無を判定し、不正と判定された場合に、当該クライアントファイアウォール間コネクションを切断し、

不正なしと判定された場合に、未結合のファイアウォールサーバ間コネクションと結合し、当該メッセージを当該ファイアウォールサーバ間コネクションを通じて前記サーバへ転送することを特徴とする請求項1に記載のネットワークサービス中継方法。

3

【請求項9】 前記第3のステップは、前記クライアントファイアウォール間コネクションとファイアウォールサーバ間コネクションとの結合状態で、前記クライアントファイアウォール間コネクションを通じて前記クライアントからの追加のメッセージを受信した場合に、このメッセージを検証して不正の有無を判定し、不正と判定された場合に、当該クライアントファイアウォール間コネクション及び当該クライアントファイアウォール間コネクションと結合済みのファイアウォールサーバ間コネクションを切断し、不正なしと判定された場合に、受信した追加のメッセージを当該クライアントファイアウォール間コネクションと結合しているファイアウォールサーバ間コネクションを通じて前記サーバへ転送し、不正ではないが、追加のメッセージでないと判定された場合に、受信したメッセージを当該クライアントファイアウォール間コネクションと結合しているファイアウォールサーバ間コネクションを通じてそのままサーバへ転送することを特徴とする請求項8に記載のネットワークサービス中継方法。

【請求項10】 前記第3のステップは、前記クライアントファイアウォール間コネクションとファイアウォールサーバ間コネクションとの結合状態で、前記ファイアウォールサーバ間コネクションを通じて前記サーバからのメッセージを受信した場合に、このメッセージを検証して不正の有無を判定し、不正と判定された場合に、当該ファイアウォールサーバ間コネクション及び当該ファイアウォールサーバ間コネクションと結合済みのクライアントファイアウォール間コネクションを切断し、不正なしと判定された場合に、当該ファイアウォールサーバ間コネクションと結合しているクライアントファイアウォール間コネクションを通じて前記クライアントへメッセージを転送し、不正ではないがメッセージでないと判定された場合に、当該ファイアウォールサーバ間コネクションと結合しているクライアントファイアウォール間コネクションを通じてそのまま前記クライアントへ転送することを特徴とする請求項1に記載のネットワークサービス中継方法。

【請求項11】 前記管理収容本数を、前記サーバからの制御信号により指定・変更することを特徴とする請求項3、4、5のいずれかに記載のネットワークサービス中継方法。

【請求項12】 前記管理収容本数を、一つ以上のクライアントをまとめた複数のクライアントグループが存在するとき、クライアントグループごとに指定・変更することを特徴とする請求項3、4、5のいずれかに記載のネットワークサービス中継方法。

【請求項13】 前記管理収容本数を、一つ以上のサ

4

バをまとめた複数のサーバグループが存在するとき、サーバグループごとに指定・変更することを特徴とする請求項3、4、5のいずれかに記載のネットワークサービス中継方法。

【請求項14】 サーバ・クライアントサービスが行われるネットワークシステムに適用され、サーバコンピュータとクライアントコンピュータとの間で伝送される情報を中継し、ファイアウォールとして機能するネットワークサービス中継装置であって、

- 10 前記サーバコンピュータとの間で予め決められた本数で、クライアントファイアウォール間コネクションと未結合のファイアウォールサーバ間コネクションを確立し管理する未結合コネクション管理手段と、前記クライアントコンピュータのうち新規にコネクション要求のあったクライアントコンピュータとの間でクライアントファイアウォール間コネクションを確立する新規コネクション処理手段と、前記新規コネクション処理手段で確立されたクライアントファイアウォール間コネクションにより結合されたクライアントコンピュータからのサービス要求について正当性を検証するサービス要求正当性検証手段と、前記サービス要求正当性検証手段で正当性が認められたとき、前記クライアントファイアウォール間コネクションとファイアウォールサーバ間コネクションとを結合して被検証サービス要求をサーバコンピュータに転送し、正当性が認められないとき、前記クライアントファイアウォール間コネクションとファイアウォールサーバ間コネクションとの結合を切断するコネクション間中継処理手段とを具備することを特徴とするネットワークサービス中継装置。
- 20
- 30

【請求項15】 さらに、前記コネクション間中継処理手段でクライアントファイアウォール間コネクションとファイアウォールサーバ間コネクションとの結合によりサーバコンピュータから送出されるサービス応答について正当性を検証するサービス応答検証手段を備え、前記コネクション間中継処理手段は、前記サービス応答検証手段で正当性が認められたとき、被検証サービス要求をクライアントコンピュータに転送し、正当性が認められないとき、前記クライアントファイアウォール間コネクションとファイアウォールサーバ間コネクションとの結合を切断することを特徴とする請求項14にネットワークサービス中継装置。

【請求項16】 前記未結合コネクション管理手段は、ファイアウォールサーバ間コネクションの最大収容本数が指定されているとき、クライアントファイアウォール間コネクションと未結合のファイアウォールサーバ間コネクション数を最大収容本数以内に制限することを特徴とする請求項14に記載のネットワークサービス中継装置。

50 【請求項17】 前記ネットワークシステムがTCP／

IP (Transport Communication Protocol/Internet Protocol) で構築されているとき、

前記コネクション間中継処理手段は、TCP層とIP層との間に配置され、前記未結合コネクション管理手段及び新規コネクション処理手段はTCP層に配置され、前記サービス要求正当性検証手段はアプリケーション層に配置されることを特徴とする請求項14に記載のネットワークサービス中継装置。

【請求項18】 前記ネットワークシステムがTCP/IP (Transport Communication Protocol/Internet Protocol) で構築されているとき、

前記コネクション間中継処理手段は、TCP層とIP層との間に配置され、前記未結合コネクション管理手段及び新規コネクション処理手段はTCP層に配置され、前記サービス要求正当性検証手段及びサービス応答正当性検証手段はアプリケーション層に配置されることを特徴とする請求項14に記載のネットワークサービス中継装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、任意の二つのコンピュータ間で確立可能なネットワークにおいて、あるコンピュータによって提供されるサービスを、ファイアウォールを介して他のコンピュータに提供するネットワークサービス中継方法及び中継装置に関する。

【0002】

【従来の技術】 コンピュータネットワーク上の2つのコンピュータ間でコネクションを確立するためのネットワークプロトコルの標準として、TCP (Transport Communication Protocol: 伝送制御プロトコル) <RFC 761参照>がある。TCPでは、「3ウェイ・ハンドシェイク」という方法でコネクションを確立する。図6にその様子を示す。

【0003】 ここで、TCPパケットのヘッダには、データパケットでデータの番号を表すSEQ (シーケンス) 番号、正常に受け取ったデータの次のデータを要求するACK (確認応答) 番号、SYN (同期) フラグ、ACKフラグなどが含まれており、TCPコネクションの確立に使われる。

【0004】 TCPでコネクションを確立する際には、まず、クライアント (C) からサーバ (S) に対してSYNパケット (P1) を送る。SYNパケット (P1) にはクライアントが無作為に決定した初期SEQ番号「CS」が含まれており、同時にSYNフラグを有効とすることで、コネクションの確立を要求していることを表している。

【0005】 サーバ (S) は、クライアント (C) からのSYNパケット (P1) が到着すると、そのクライアント (C) に対してSYNパケット (P1) を受け取ったことを伝えるために、SYN/ACKパケット (P

2) を生成してクライアント (C) へ送る。このSYN/ACKパケット (P2) の生成では、クライアント (C) からのSEQ番号に1を加えた値「CS+1」をACK番号に設定し、ACKフラグを有効にすると同時に、サーバ (S) 自身が無作為に決定した初期SEQ番号「SS」を設定してSYNフラグを有効にしている。

【0006】 クライアント (C) では、サーバ (S) からSYN/ACKパケット (P2) を受け取った時点でコネクションが確立する。但し、サーバ (S) 側ではまだコネクションが確立していないので、クライアント (C) はACKパケット (P3) を生成してサーバ (S) に送る。このACKパケット (P3) の生成では、SEQ番号にサーバ (S) から送られてきたSYN/ACKパケット (P2) のACK番号に示された番号「CS+1」を設定し、ACK番号にSYN/ACKパケット (P2) のSEQ番号に1を加えた値「SS+1」を設定している。

【0007】 サーバ (S) 側にこのACKパケット (P3) が到着した時点で、クライアント (C) とサーバ (S) 両側のSEQ番号が同期され、サーバ (S) 側でもコネクションが確立する。コネクション確立後はクライアント (C)、サーバ (S) のいずれの側からでもデータを送ることができる。

【0008】 例えば、クライアント (C) からサーバ (S) へ最初のデータを送る際には、SEQ番号には「CS+1」を設定し、ACK番号には「SS+1」を設定して、ACKフラグを有効にしたデータパケット (P4) を送る。さらに、追加のデータを送る際には、先程送った100bytesのデータの次を表すSEQ番号「CS+101」、ACK番号には「SS+1」を設定してACKフラグを有効にしたデータパケット (P5) を送る。

【0009】 データを受け取ったサーバ (S) はクライアント (C) に対して適当なタイミングでACKパケット (P6) を送る。この際のACKパケット (P6) を送る場合には、ACK番号にその時点で受信済みのデータ (SEQ番号でCS+250) の次のSEQ番号を表す「CS+251」を設定し、SEQ番号に「SS+1」を設定し、ACKフラグを有効にする。

【0010】 コンピュータネットワークでは、ネットワークを通じてサービスを提供するサーバとサービスを受けるクライアントがある。HTTP (ハイパーテキスト転送プロトコル) <RFC 1945参照>に基づくWWW (World Wide Web) サーバとWWWブラウザ、FTP (ファイル転送プロトコル) <RFC 959参照>に基づくFTPサーバとFTPクライアントなどはその好例である。

【0011】 ところで、上記のようなサービスをネットワーク上で提供するサーバとして動作させているサーバコンピュータは、侵入やサービス拒否攻撃 (Denial of

10

20

30

40

50

Service Attack)などの攻撃を受けることが多い。このような攻撃からサーバコンピュータを守る手段として、ファイアウォールをサーバコンピュータの手前に設置する方法がある。

【0012】このファイアウォールでサーバコンピュータを守る手法には、大きくわけて「パケット・フィルタリング」と「アプリケーション・ゲートウェイ」の二種類がある。

【0013】前者の「パケット・フィルタリング」は、ネットワークを通じて通信を行う単位であるパケットを10 チェックすることでサーバを守るようにした手法である。すなわち、パケットには宛先となるコンピュータのIPアドレスとサービス種別を表すポート番号が含まれていることに着目し、特定のIPアドレスとポート番号の組み合わせを持つパケットのみを通すようにした手法である。例えば、IPアドレスが(10.0.0.1)のサーバコンピュータでWWWサービスを提供したい場合は、サーバコンピュータのIPアドレスである(10.0.0.1)とWWWサービスのポート番号である(80)を持つパケットだけを通すように設定する。

【0014】後者の「アプリケーション・ゲートウェイ」は、ファイアウォールがクライアントからのサービス要求などのメッセージを全て受け取って、サービスのルールに従っているかどうかを判断し、ルールに従っている場合は、同じ内容のサービス要求を作ってサーバコンピュータへ転送し、当該サーバコンピュータからの返答をクライアントへ中継するという手法である。

【0015】

【発明が解決しようとする課題】しかしながら、従来のファイアウォールの「パケット・フィルタリング」による手法では、パケットをチェックするだけなので、アプリケーションレベルのサービス要求が不正であったりする場合これをチェックすることができない。例えば、WWWサーバへのサービス拒否攻撃を行う場合はWWWクライアントからのWWWサービス要求の形をとる場合が多いが、このような攻撃は「パケット・フィルタリング」では防ぐことができない。また、大量の接続確立要求をサーバに要求するという方式のサービス拒否攻撃も「パケット・フィルタリング」では防げない。

【0016】他方の「アプリケーション・ゲートウェイ」による手法であれば、クライアントのサービス要求がサービスのルールに従っているかどうかを判断するので、上記の例のようなサービス拒否攻撃を防ぐことができる。しかしながら、「アプリケーション・ゲートウェイ」はサーバとクライアントの間にたって互いの間の通信を中継する形となり、通常はOS(Operating System)の上のアプリケーションとして実現されているので、前者の「パケット・フィルタリング」と比べると、クライアントがサービス要求を送信してからサーバからの返答を受信するまでの応答時間が長くなってしまふ。

【0017】本発明は、上記の問題を解決するためになされたもので、その目的とするところは、「アプリケーション・ゲートウェイ」と同様にサービス要求の正当性まで判断する能力と「パケット・フィルタリング」と同等の応答時間の短さを兼ね備えるファイアウォールを構築したネットワークサービス中継方法及び中継装置を提供することにある。

【0018】また、本発明の他の目的は、上記ネットワークサービス中継方法及び中継装置において、ファイアウォールがサーバの代わりにクライアントとの間にコネクションを確立することができ、これによって新規コネクション確立にかかるサーバの負担を軽減することにある。

【0019】また、本発明の他の目的は、上記ネットワークサービス中継方法及び中継装置において、ファイアウォールがサーバとクライアントとの間のコネクションの数を管理することができ、これによってサービス提供にかかるサーバの負荷を管理することにある。

【0020】

20 【課題を解決するための手段】上記の目的を達成するために本発明に係るネットワークサービス中継方法は、以下のような特徴的構成を備える。

【0021】(1)任意の二つのコンピュータ間でのコネクションを双方のコネクションキーに基づいて確立可能なネットワークに適用され、あるコンピュータ上のサーバによって提供されるサービスを、そのコンピュータとは別のコンピュータ、もしくは同一のコンピュータによって提供されるファイアウォールを介して、他のコンピュータ上のクライアントに提供するネットワークサービス中継方法であって、前記ファイアウォールと前記サーバとの間に予め1本以上のファイアウォール-サーバ間コネクションを確立し、前記コネクションに用いられた前記サーバ側と前記ファイアウォール側のコネクションキーを保持しておく第1のステップと、前記クライアントと前記ファイアウォールとの間に第1のステップで保持しておいた前記サーバ側コネクションキーの一つを用いてクライアント-ファイアウォール間コネクションを確立し、前記コネクションの確立に用いられた前記クライアント側のコネクションキーと前記ファイアウォール側のコネクションキーを保持する第2のステップと、前記クライアント-ファイアウォール間コネクションと前記ファイアウォール-サーバ間コネクションとを結合・中継する第3のステップとを具備することを特徴とする。

40 50 【0022】(2)(1)の構成において、前記第3のステップは、前記クライアントから届くメッセージのコネクションキーを前記ファイアウォール-サーバ間コネクションの前記ファイアウォール側のコネクションキーに書き換えて前記サーバへ転送し、前記サーバから届くメッセージのコネクションキーを前記クライアント-フ

ファイアウォール間コネクションの前記クライアント側のコネクションキーに書き換えて前記クライアント側へ転送することを特徴とする。

【0023】(3)(1)の構成において、前記第1のステップは、予め管理収容本数として整数 M ($M \geq 1$) が指定されているとき、前記クライアントファイアウォール間コネクションと未結合のファイアウォールサーバ間コネクションと、クライアントファイアウォール間コネクションと結合済みのファイアウォールサーバ間コネクションを合わせた、ファイアウォールサーバ間コネクションの合計が M 本以下となるように、ファイアウォールサーバ間コネクションの確立を制限することを特徴とする。

【0024】(4)(3)の構成において、前記第1のステップは、予め初期の管理収容本数として整数 N ($M \geq N \geq 1$) が指定されているとき、初期状態で N 本の未結合ファイアウォールサーバ間コネクションを確立する初期化処理を実行することを特徴とする。

【0025】(5)(4)の構成において、前記第1のステップは、前記ファイアウォールサーバ間コネクションの合計が M 本以下のとき、前記未結合ファイアウォールサーバ間コネクションの切断または前記クライアントファイアウォール間コネクションとの結合により前記未結合ファイアウォールサーバ間コネクションが N 本より少なくなった場合に、新たに未結合ファイアウォールサーバ間コネクションを確立して、 N 本の未結合ファイアウォールサーバ間コネクションを維持することを特徴とする。

【0026】(6)(1)の構成において、前記第2のステップは、前記ファイアウォールサーバ間コネクションと結合していない未結合のクライアントファイアウォール間コネクションと、前記ファイアウォールサーバ間コネクションと結合済みのファイアウォールクライアント間コネクションとを合わせた、クライアントファイアウォール間コネクションの合計が、前記第1のステップで確立されている前記ファイアウォールサーバ間コネクションの合計を上回らないように、クライアントファイアウォール間コネクションの確立を制限することを特徴とする。

【0027】(7)(1)の構成において、前記第2のステップは、新たにクライアントからファイアウォールに対してコネクション確立要求があった場合に、前記未結合ファイアウォールサーバ間コネクションの数と前記未結合クライアントファイアウォール間コネクションの数を比較し、サーバ側コネクション数よりクライアント側コネクション数が上回っていれば、新たにクライアントファイアウォール間コネクションを確立し、クライアント側コネクション数がサーバ側コネクション数と同数か下回るようであれば、クライアントからのコネクション確立要求を廃棄するか、あるいは、前記未結合

ファイアウォールサーバ間コネクションの数が前記未結合クライアントファイアウォール間コネクションの数を上回るまでクライアントファイアウォール間コネクション確立を遅延することを特徴とする。

【0028】(8)(1)の構成において、前記第3のステップは、前記クライアントファイアウォール間コネクションとファイアウォールサーバ間コネクションとの結合状態で、前記クライアントファイアウォール間コネクションを通じて前記クライアントからのメッセージを受信した場合に、このメッセージを検証して不正の有無を判定し、不正と判定された場合に、当該クライアントファイアウォール間コネクションを切断し、不正なしと判定された場合に、未結合のファイアウォールサーバ間コネクションと結合し、当該メッセージを当該ファイアウォールサーバ間コネクションを通じて前記サーバへ転送することを特徴とする。

【0029】(9)(8)の構成において、前記第3のステップは、前記クライアントファイアウォール間コネクションとファイアウォールサーバ間コネクションとの結合状態で、前記クライアントファイアウォール間コネクションを通じて前記クライアントからの追加のメッセージを受信した場合に、このメッセージを検証して不正の有無を判定し、不正と判定された場合に、当該クライアントファイアウォール間コネクション及び当該クライアントファイアウォール間コネクションと結合済みのファイアウォールサーバ間コネクションを切断し、不正なしと判定された場合に、受信した追加のメッセージを当該クライアントファイアウォール間コネクションと結合しているファイアウォールサーバ間コネクションを通じて前記サーバへ転送し、不正ではないが、追加のメッセージでないと判定された場合に、受信したメッセージを当該クライアントファイアウォール間コネクションと結合しているファイアウォールサーバ間コネクションを通じてそのままサーバへ転送することを特徴とする。

【0030】(10)(1)の構成において、前記第3のステップは、前記クライアントファイアウォール間コネクションとファイアウォールサーバ間コネクションとの結合状態で、前記ファイアウォールサーバ間コネクションを通じて前記サーバからのメッセージを受信した場合に、このメッセージを検証して不正の有無を判定し、不正と判定された場合に、当該ファイアウォールサーバ間コネクション及び当該ファイアウォールサーバ間コネクションと結合済みのクライアントファイアウォール間コネクションを切断し、不正なしと判定された場合に、当該ファイアウォールサーバ間コネクションと結合しているクライアントファイアウォール間コネクションを通じて前記クライアントへメッセージを転送し、不正ではないがメッセージでないと判定された場合に、当該ファイアウォールサーバ間コネクション

と結合しているクライアントファイアウォール間コネクションを通じてそのまま前記クライアントへ転送することを特徴とする。

【0031】(11)(3)、(4)、(5)のいずれかの構成において、前記管理収容本数を、前記サーバからの制御信号により指定・変更することを特徴とする。

【0032】(12)(3)、(4)、(5)のいずれかの構成において、前記管理収容本数を、一つ以上のクライアントをまとめた複数のクライアントグループが存在するとき、クライアントグループごとに指定・変更することを特徴とする。

【0033】(13)(3)、(4)、(5)のいずれかの構成において、前記管理収容本数を、一つ以上のサーバをまとめた複数のサーバグループが存在するとき、サーバグループごとに指定・変更することを特徴とする。

【0034】また、本発明に係るネットワークサービス中継装置は、以下のような特徴的構成を備える。

【0035】(14)サーバ・クライアントサービスが行われるネットワークシステムに適用され、サーバコンピュータとクライアントコンピュータとの間で伝送される情報を中継し、ファイアウォールとして機能するネットワークサービス中継装置であって、前記サーバコンピュータとの間で予め決められた本数で、クライアントファイアウォール間コネクションと未結合のファイアウォールサーバ間コネクションを確立し管理する未結合コネクション管理手段と、前記クライアントコンピュータのうち新規にコネクション要求のあったクライアントコンピュータとの間でクライアントファイアウォール間コネクションを確立する新規コネクション処理手段と、前記新規コネクション処理手段で確立されたクライアントファイアウォール間コネクションにより結合されたクライアントコンピュータからのサービス要求について正当性を検証するサービス要求正当性検証手段と、前記サービス要求正当性検証手段で正当性が認められたとき、前記クライアントファイアウォール間コネクションとファイアウォールサーバ間コネクションとを結合して被検証サービス要求をサーバコンピュータに転送し、正当性が認められないとき、前記クライアントファイアウォール間コネクションとファイアウォールサーバ間コネクションとの結合を切断するコネクション間中継処理手段とを具備することを特徴とする。

【0036】(15)(14)の構成において、さらに、前記コネクション間中継処理手段でクライアントファイアウォール間コネクションとファイアウォールサーバ間コネクションとの結合によりサーバコンピュータから送出されるサービス応答について正当性を検証するサービス応答検証手段を備え、前記コネクション中継処理手段は、前記サービス応答検証手段で正当性が認められたとき、被検証サービス要求をクライアントコンピ

ュータに転送し、正当性が認められないとき、前記クライアントファイアウォール間コネクションとファイアウォールサーバ間コネクションとの結合を切断することを特徴とする。

【0037】(16)(14)の構成において、前記未結合コネクション管理手段は、ファイアウォールサーバ間コネクションの最大収容本数が指定されているとき、クライアントファイアウォール間コネクションと未結合のファイアウォールサーバ間コネクション数を最大収容本数以内に制限することを特徴とする。

【0038】(17)(14)の構成において、前記ネットワークシステムがTCP/IP (Transport Communication Protocol/Internet Protocol) で構築されているとき、前記コネクション間中継処理手段は、TCP層とIP層との間に配置され、前記未結合コネクション管理手段及び新規コネクション処理手段はTCP層に配置され、前記サービス要求正当性検証手段はアプリケーション層に配置されることを特徴とする。

【0039】(18)(14)の構成において、前記ネットワークシステムがTCP/IP (Transport Communication Protocol/Internet Protocol) で構築されているとき、前記コネクション間中継処理手段は、TCP層とIP層との間に配置され、前記未結合コネクション管理手段及び新規コネクション処理手段はTCP層に配置され、前記サービス要求正当性検証手段及びサービス応答正当性検証手段はアプリケーション層に配置されることを特徴とする。

【0040】本発明は、以上の構成によって、サービス要求の正当性を判断した上でサービス中継を高速に行うことができ、クライアントとのコネクションの確立にかかる負担を軽減し、クライアントとサーバとのコネクションの数を管理できるファイアウォールを実現する技術を提供する。

【0041】

【発明の実施の形態】以下、図1乃至図5を参照して本発明の実施の形態を詳細に説明する。

【0042】図1は、本発明が適用されるTCPネットワークシステムの構成を示す概念図である。図1において、11はネットワークN1に接続され、サーバ(S)として機能するサーバコンピュータ、12はネットワークN2に接続され、クライアント(C)として機能するクライアントコンピュータであり、ネットワークN1とネットワークN2を接続する経路には、ファイアウォール(F)として機能する結合・中継モジュール13が介在される。

【0043】以下、上記システムに本発明を適用した場合の第1乃至第3の実施形態を説明する。

【0044】(第1の実施形態)第1の実施形態として、本発明に係るサービス中継方法をシーケンス処理によって実現する場合について、図2に示すシーケンス図

を参照して説明する。

【0045】図2において、まずファイアウォール(F)は、予めサーバ(S)との間でSYNパケット(P11)、SYN/ACKパケット(P12)、ACKパケット(P13)のやり取りを通じてファイアウォール-サーバ間コネクションを確立しておく。

【0046】上記ファイアウォール(F)は、クライアント(C)からのコネクション確立要求に基づくSYNパケット(P14)を受けると、SYN/ACKパケット(P15)、ACKパケット(P16)のやり取りを通じてクライアント-ファイアウォール間コネクションを確立する。この際、ファイアウォール(F)が使用するSEQ番号は、サーバ(S)とのファイアウォール-サーバ間コネクションの確立時に当該サーバ(S)が用いた初期SEQ番号「SS」を使用する。

【0047】その後、ファイアウォール(F)は、クライアント(C)からのデータパケット(P17)を受け取ると、そのSEQ番号「CS+1」を、ファイアウォール(F)が確立したファイアウォール-サーバ間コネクションの初期SEQ番号「FW」に基づいてSEQ番号「FW+1」に書き換え、そのデータパケット(P18)をサーバ(S)へ中継転送する。続いて、サーバ(S)からのACKパケット(P19)のACK番号「FW+101」をクライアントの初期SEQ番号に基づいたACK番号「CS+101」へ書き換え、そのデータパケット(P20)をクライアント(C)へ中継転送することにより実現する。

【0048】上記処理におけるファイアウォール(F)での処理を図3に示す。

【0049】まず、ファイアウォール(F)は、初期設定として、サーバ(S)との間に新しいファイアウォール-サーバ間コネクションを確立しておき、ファイアウォール(F)側とサーバ(S)側の初期SEQ番号「FW」、「SS」を保持し(S1)、次にクライアント(C)から接続要求が来るまで待機する(S2)。クライアント(C)から接続要求があれば、保持しておいたサーバ側初期SEQ番号「SS」をクライアント(C)とのコネクション確立に用いてクライアント-ファイアウォール間コネクションを確立し、クライアント側初期SEQ番号「CS」を保持し(S3)、一定期間、クライアント(C)からのTCPデータパケット到着を待機する(S4)。

【0050】一定期間内にクライアント(C)からTCPデータパケットが到着した場合、そのTCPデータパケットはクライアント-ファイアウォール間コネクションのクライアント側初期SEQ番号「CS」を元にした「CS+ Δ CS」をSEQ番号としているので、これをファイアウォール-サーバ間コネクションのファイアウォール側初期SEQ番号「FW」を元としたSEQ番号「FW+ Δ CS」に書き換えてからサーバ(S)へTC

Pデータパケットを転送する(S5)。転送後、ステップS4に戻る。

【0051】ステップS4において、一定期間内にクライアント(C)からTCPデータパケットが到着しなかった場合、さらに一定期間、サーバ(S)からのTCPデータパケット到着を待機する(S6)。一定期間内にサーバ(S)からTCPデータパケットが到着した場合、そのTCPデータパケットはファイアウォール-サーバ間コネクションのファイアウォール側初期SEQ番号「FW」を元とした「FW+ Δ FW」をACK番号としているので、これをクライアント-ファイアウォール間コネクションのクライアント側SEQ番号「CS」を元とした「CS+ Δ CS」に書き換えてからクライアント(C)へTCPデータパケットを転送する(S7)。転送後、ステップS4に戻る。

【0052】ステップS6において、一定期間内にサーバ(S)からTCPデータパケットが到着しなかった場合、タイムアウトか接続先コンピュータからの要求で、ファイアウォール-サーバ間コネクション、クライアント-ファイアウォール間コネクションのいずれかが切断されたか判断する(S8)。切断されていなければステップS4に戻る。切断されている場合には、他方のコネクションを切断して、保持しておいた各初期SEQ番号「FW」、「SS」、「CS」をクリアし(S9)、ステップS1に戻る。

【0053】上記処理の結果、ファイアウォール(F)において、予めサーバ(S)との接続を確保しておくことで、クライアント(C)からの接続時のサーバ(S)への負荷軽減と、サーバ(S)とクライアント(C)との間のTCPデータパケット中継時におけるSEQ番号およびACK番号の書き換えのみによる中継処理の高速化を実現することができる。

【0054】(第2の実施形態)第2の実施形態として、本発明に係るサービス中継方法を図1に示した結合・中継モジュール13に適用した場合について、図4に示す概念図を参照して説明する。

【0055】図4に示す結合・中継モジュール13は、サーバコンピュータ11とのファイアウォール-サーバ間コネクションの最大収容本数Mのうち、クライアント-ファイアウォール間コネクションと結合していないファイアウォール-サーバ間コネクション数をN本に設定し管理する未結合コネクション管理部131、ファイアウォール-サーバ間コネクションとクライアント-ファイアウォール間コネクションとの間で中継を行うコネクション間中継処理部132、クライアントコンピュータ12からの新規コネクション確立要求を処理する新規コネクション処理部133、新規コネクション確立時あるいは中継時におけるサービス要求の正当性を検証するサービス要求正当性検証部134、中継時のサービス応答の正当性を検証するサービス応答正当性検証部135か

ら構成される。

【0056】上記構成において、以下に処理の流れに沿って、その動作を説明する。

【0057】ファイアウォールを構築する結合・中継モジュール13において、未結合コネクション管理部131は、サーバコンピュータ11との間で予めN本のファイアウォール-サーバ間コネクションを確立しておき、そのコネクションキーを保持しておく。新規クライアントコンピュータ12iから接続要求があったときに、未結合コネクション数が1以上であれば、新規コネクション処理部133は、未結合コネクション管理部131に保持されているコネクションキーを用いて、クライアント-ファイアウォール間コネクションを確立させる。

【0058】次に、サービス要求正当性検証部134は、結合済みクライアントコンピュータ121~12nからのサービス要求を受けると、その正当性を検証する。また、サービス応答正当性検証部135は、サーバコンピュータ11からのサービス応答を受けると、その正当性を検証する。コネクション間中継処理部132は、サービス要求正当性検証部134、サービス応答正当性検証部135の各検証結果が正当であったときのみ、サーバコンピュータ11と結合済みクライアントコンピュータ121~12nとの間の中継を行う。

【0059】すなわち、コネクション間中継処理部132が中継するサービス要求は、サービス要求正当性検証部134が検証し、正当でなければコネクション間中継処理部132がクライアントコンピュータ側とサーバコンピュータ側のコネクションを切断し、そうでなければ中継を行う。同様にコネクション間中継処理部132が中継するサービス応答は、サービス応答正当性検証部135が検証し、正当でなければコネクション間中継処理部132がクライアントコンピュータ側とサーバコンピュータ側のコネクションを切断し、そうでなければ中継を行う。

【0060】上記のモジュール構成によれば、結果として、サーバコンピュータ11のコネクション数をM本以下に限定することができ、サーバコンピュータにかかる負荷を限定できる。また、サーバコンピュータとクライアントコンピュータ間のサービス要求及びサービス応答の正当性を検証できる。

【0061】（第3の実施形態）第3の実施形態として、図1に示すシステムがTCP/IPで構築されている場合に、本発明に係るサービス中継方法を結合・中継モジュール13のTCP/IP階層にて実現する場合について、図5に示すTCP/IP階層構造図を参照して説明する。尚、図5において、図4と同一機能を果たすブロックには同一符号を付して示す。

【0062】図5に示す階層構造では、ネットワークインタフェース層、IP層、TCP層、アプリケーション層を備え、IP層とTCP層との間にコネクション間中

継処理部132を配置し、TCP層に新規コネクション処理部131、未結合コネクション管理部133を配置し、アプリケーション層にサービス要求正当性検証部134、サービス応答正当性検証部135を配置している。

【0063】未結合コネクション管理部131は、予めサーバコンピュータ11との間でサーバ-ファイアウォール間コネクションを確立し、コネクションキーを保持しておく。クライアントコンピュータ12から新規コネクション確立要求があれば、まず、新規コネクション処理部133が未結合コネクション管理部131に保持されているコネクションキーを用いてコネクションの確立を行う。

【0064】次に、サービス要求正当性検証部134がサービス要求を検証し、正当であれば、コネクション間中継処理部132がサービス要求をサーバコンピュータ11に転送する。また、サービス応答正当性検証部135がサービス要求を検証し、正当であれば、コネクション間中継処理部132がサービス応答をクライアントコンピュータ12に転送する。以後の処理は、コネクション間中継処理部132によるパケットヘッダの書き換えだけで中継が行われる。

【0065】上記のTCP/IP階層でのモジュール構成によれば、結果として、「アプリケーション・ゲートウェイ」と同等のサービス要求の検証ができ、同時に以後の中継をパケットヘッダの書き換えだけにより行うため、「パケット・フィルタリング」と同等の応答速度を得ることができる。

【0066】尚、上記の各実施形態では、サーバコンピュータとは別にファイアウォールとして機能する結合・中継モジュールを備えるシステムに適用する場合について説明したが、サーバコンピュータ自体に各実施形態の結合・中継モジュールを組み込むことも可能である。

【0067】

【発明の効果】以上のように本発明によれば、「アプリケーション・ゲートウェイ」と同様にサービス要求の正当性まで判断する能力と「パケット・フィルタリング」と同等の応答時間の短さを兼ね備えるファイアウォールを構築したネットワークサービス中継方法及び中継装置を提供することができる。

【0068】また、上記ネットワークサービス中継方法及び中継装置において、ファイアウォールがサーバの代わりにクライアントとの間にコネクションを確立することができ、これによって新規コネクション確立にかかるサーバの負担を軽減することができる。

【0069】また、上記ネットワークサービス中継装置において、ファイアウォールがサーバとクライアントとの間のコネクションの数を管理することができ、これによってサービス提供にかかるサーバの負担を管理することができる。

【0070】結果として、「アプリケーション・ゲートウェイ」方式と同等の強固なサービス要求検証能力を持ちつつ、コネクション確立後は簡単な処理での中継が可能で、コネクション確立時のサーバへの負担が軽減し、クライアントとサーバ間のコネクション数を管理することのできるネットワークサービス中継方法及び中継装置を提供することができる。

【図面の簡単な説明】

【図1】 本発明が適用されるTCPネットワークシステムの構成を示す概念図。

【図2】 第1の実施形態として、本発明に係るサービス中継方法をシーケンス処理によって実現する場合を説明するためのシーケンス図。

【図3】 第1の実施形態のファイアウォール（F）での処理を示すフローチャート。

【図4】 第2の実施形態として、本発明に係るサービス中継方法を結合・中継モジュールに適用した場合を説明するための概念図。

【図5】 第3の実施形態として、本発明に係るサービ

ス中継方法をTCP/IPネットワークシステムにおける結合・中継モジュール13のTCP/IP階層にて実現する場合を説明するためのTCP/IP階層構造図。

【図6】 TCPのコネクション確立の様子を示すシーケンス図。

【符号の説明】

S…サーバ

C…クライアント

F…ファイアウォール

10 11…サーバコンピュータ

12…クライアントコンピュータ

13…機能する結合・中継モジュール（ファイアウォール）

131…未結合コネクション管理部

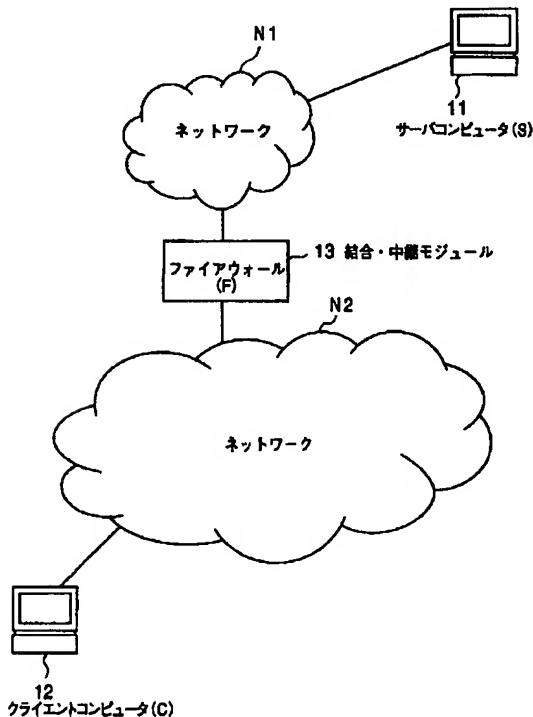
132…コネクション間中継処理部

133…新規コネクション処理部

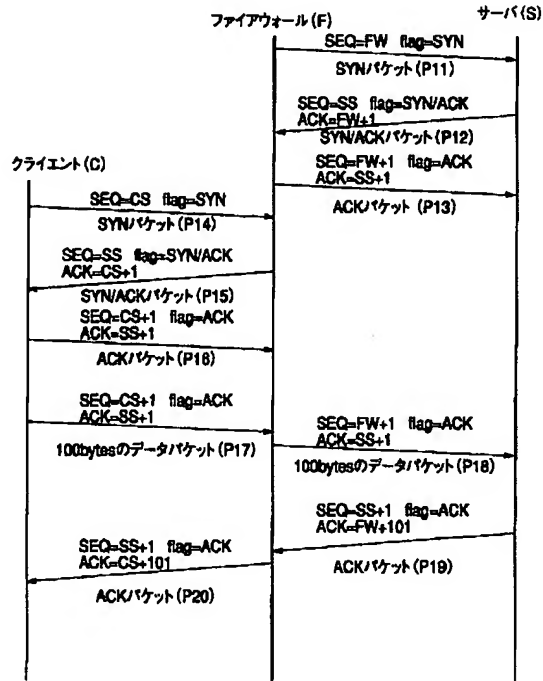
134…サービス要求正当性検証部

135…サービス応答正当性検証部

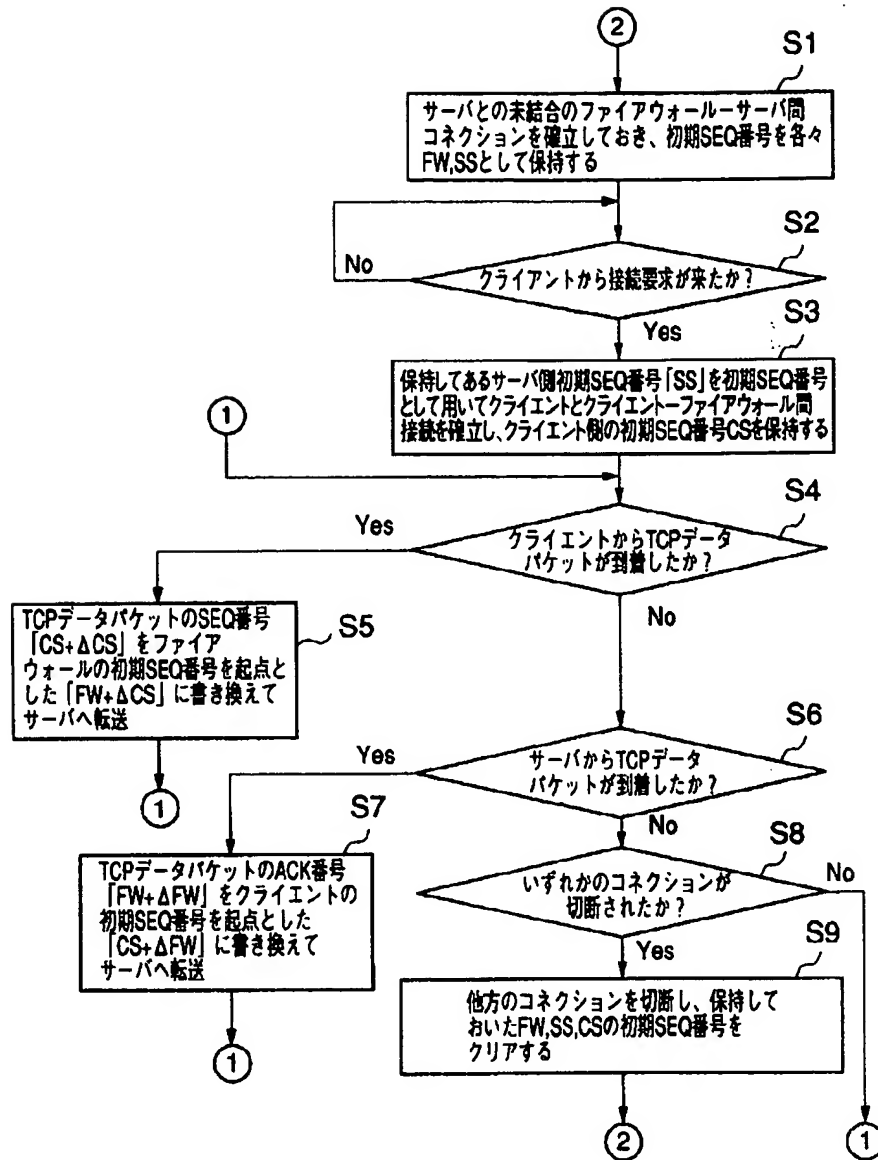
【図1】



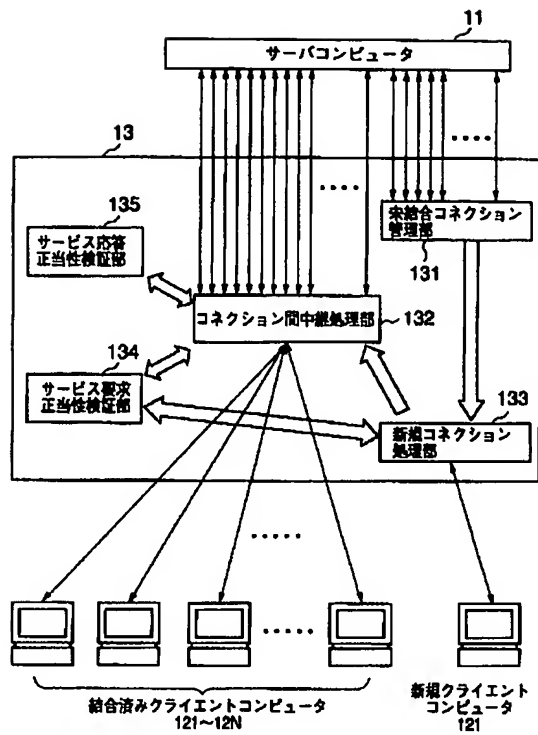
【図2】



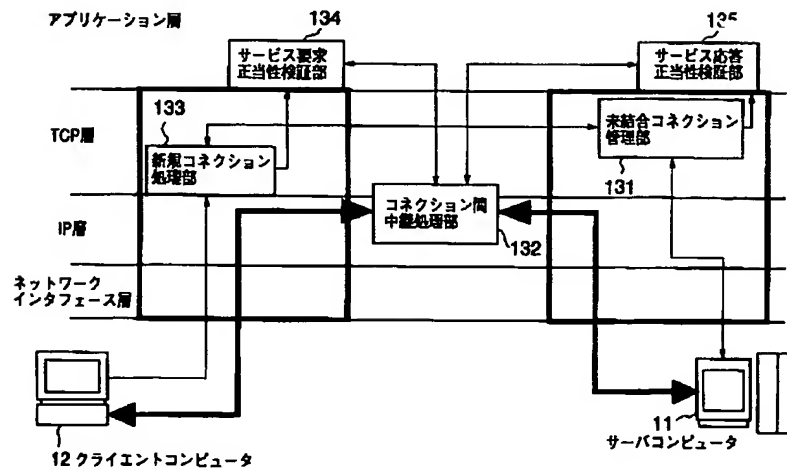
【図3】



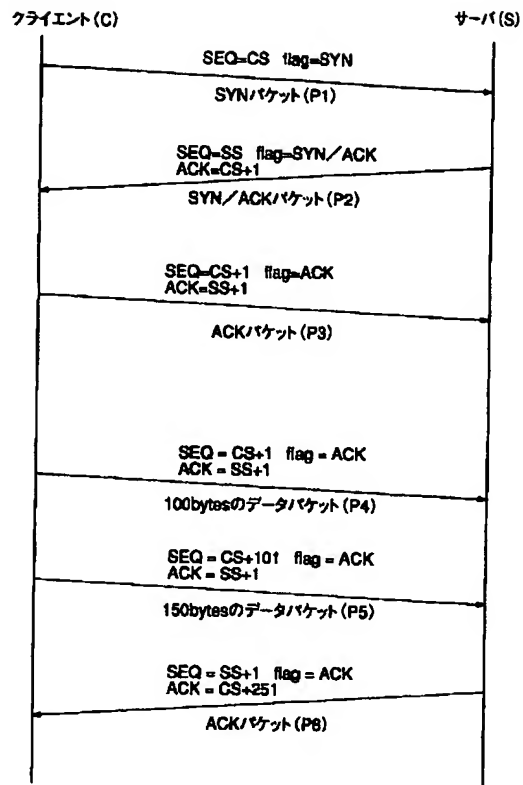
【図4】



【図5】



【図6】



フロントページの続き

(72)発明者 盛合 敏

東京都千代田区大手町二丁目3番1号 日

本電信電話株式会社内

Fターム(参考) 5B089 GA04 GB01 HB18 KA05 KA17

KB13 KG03 KG07

5K030 GA02 GA15 HA08 HD03 JA11

JT06 LB01 LB19

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.